The Chromium mess meets Android

Proposals on how to get a fully free WebView build or replace it with something completely new

David Ludovino Jeremy Rand *

Replicant

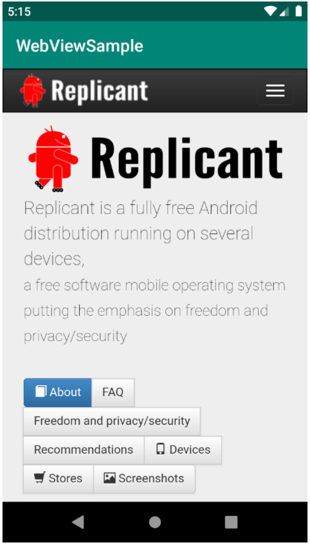
* with support from Andrés D and Kurtis Hanna

What is WebView?

Renders web content (HTML, CSS, JavaScript) inside apps.

API has been around since Android 1.

```
public class MainActivity extends Activity {
  @Override
  protected void onCreate(Bundle state) {
    super.onCreate(state);
    WebView v = new WebView(this);
    setContentView(v);
    v.loadUrl("https://replicant.us");
  }
}
```



5:15

WebViewSample

Replicant

Replicant

Replicant is a fully free Android distribution running on several devices,

a free software mobile operating system putting the emphasis on freedom and privacy/security

Which apps use WebView?

Apps that render HTML: email clients, RSS readers, etc.

Became pervasive with the advent of cross-platform mobile frameworks.

Half of the apps listed at PRISM Break depend on WebView

uses WebView					does not use WebView				
K-9 Mail	OsmAnd	Nextcloud	Tiny Tiny RSS	I2P	Orbot	F-Droid	andOTP	Shaarlier	Briar
wallabag	OpenKeychain	EteSync	Syncthing	Signal	Conversations	Silence	Tinc App	KeePass DX	Jami
dandelion*	Nomad	Tusky	Movim		Bitmask	Wireguard	Fennec F-Droid	Tor Browser	Thorium

What is underneath WebView?

WebKit until Android 4.3 Jelly Bean (API 18).

Chromium from Android 4.4 KitKat (API 19) onwards.

What's the matter with Chromium?

Privacy issues:

- Background requests to Google during build and run.
- Depends on Google services for several features (e.g. Safe Browsing).
- Limited privacy controls.
- API prevents extensions from blocking ads.

What's the matter with Chromium?

Privacy issues:

- Background requests to Google during build and run.
- Depends on Google services for several features (e.g. Safe Browsing).
- Limited privacy controls.
- API prevents extensions from blocking ads.

Security issues:

- Prevents users from escaping the certificate authority system for TLS.

What's the matter with Chromium?

Privacy issues:

- Background requests to Google during build and run.
- Depends on Google services for several features (e.g. Safe Browsing).
- Limited privacy controls.
- API prevents extensions from blocking ads.

Security issues:

- Prevents users from escaping the certificate authority system for TLS.

Freedom issues:

- Pre-built binaries throughout the code base.
- Missing license in some source files.

What's the matter with Chromium?

Privacy issues:

- Background requests to Google during build and run.
- Depends on Google services for several features (e.g. Safe Browsing).
- Limited privacy controls.
- API prevents extensions from blocking ads.

Security issues:

- Prevents users from escaping the certificate authority system for TLS.

Freedom issues:

- Pre-built binaries throughout the code base.
- Missing license in some source files.

Verdict: unfit for fully free-software distributions.

WebView and Replicant

Replicant:

- Android distribution
- compliant with GNU Free System Distribution Guidelines (FSDG)

Using outdated WebView based on Chromium 43: lots of security concerns.

How to create a WebView build that respects user's privacy and freedom?

Desktop Chromium forks

- ungoogled-chromium: aligned with privacy and freedom
- Bromite: can build WebView; only focused on privacy and ad blocking
- Debian: replaces pre-builts with system libs; Google services not removed
- Iridium: one step on every direction; not as thorough as others

Guix, a FSDG compliant distro, uses:
ungoogled-chromium + build recipe that removes some files.

Android Chromium forks

Android builds require many more pre-builts and proprietary dependencies. E.g.: Google Mobile Services (GMS)

- ungoogled-chromium-android: ungoogled-chromium + Android specific patches; has some remaining pre-builts
- Unobtainium: aimed to be built within F-Droid (forbids pre-builts); project is unmaintained

Android Chromium forks

strings classes.dex | grep google

Chromium 78 WebView - 227 lines

```
.  You must have the following declaration within the <application> element:
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version" />
Google Inc.1
Google Inc.1
Google Inc.1
A required meta-data tag in your app's AndroidManifest.xml does not exist.
You must have the following declaration within the <application> element:
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version" />
RCompositeGoogleApiClient should not be used without any APIs that require sign-in.
OConnection timed out while waiting for Google Play services update to complete.
+Failed to connect to Google Play Services:
-Failed to get Google certificates from remote
Google Play Services
"Google Play Services not available
Google Play Store is missing.
$Google Play Store signature invalid.
OGoogle Play services is invalid. Cannot recover.
 Google Play services is missing.
;Google Play services missing when getting application info.
,Google Play services out of date.  Requires
'Google Play services signature invalid.
GoogleApiActivity
GoogleApiAvailability
&GoogleApiClient connecting is in step
)GoogleApiClient is not configured to use
HGoogleApiClient is not configured to use the API required for this call.
GoogleApiClient is not configured to use the LocationServices.API Api. Pass thisinto GoogleApiClient.Builder#addApi() to use
%GoogleApiClient is not connected yet.
 GoogleApiClient must not be null
&GoogleApiClient parameter is required.
GoogleApiClient received too many callbacks for the given step. Clients may be in an unexpected state; GoogleApiClient will
GoogleApiClientConnecting
GoogleApiClientImpl
GoogleApiHandler
GoogleApiManager
GoogleCertificates
/GoogleCertificates has been initialized already
```

Android Chromium forks

```
strings classes.dex | grep google
```

Bromite 78 WebView - 124 lines

```
.  You must have the following declaration within the <application> element:
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version" />
Google Inc.1
Google Inc.1
Google Inc.1
A required meta-data tag in your app's AndroidManifest.xml does not exist.
You must have the following declaration within the <application> element:
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version" />
0Connection timed out while waiting for Google Play services update to complete.
-Failed to get Google certificates from remote
Google Play Store is missing.
$Google Play Store signature invalid.
0Google Play services is invalid. Cannot recover.
 Google Play services is missing.
;Google Play services missing when getting application info.
,Google Play services out of date.  Requires
'Google Play services signature invalid.
GoogleApiActivity
GoogleApiAvailability
GoogleApiHandler
GoogleApiManager
GoogleCertificates
/GoogleCertificates has been initialized already
GooglePlayServicesErrorDialog
GooglePlayServicesUtil
GoogleSignatureVerifier
<Lcom/google/android/gms/auth/api/signin/GoogleSignInAccount;
0Lcom/google/android/gms/common/ConnectionResult;
'Lcom/google/android/gms/common/Feature;
3Lcom/google/android/gms/common/annotation/KeepName;
5Lcom/google/android/gms/common/api/GoogleApiActivity;
)Lcom/google/android/gms/common/api/Scope;
*Lcom/google/android/gms/common/api/Status;
>Lcom/google/android/gms/common/api/internal/BasePendingResult;
>Lcom/google/android/gms/common/api/internal/LifecycleCallback;
6Lcom/google/android/gms/common/internal/BaseGmsClient;
7Lcom/google/android/gms/common/internal/ConnectionInfo;
```

Android Chromium forks

```
strings classes.dex | grep google
```

ungoogled-chromium-android 77 WebView - 10 lines

```
OMX.google.
OMX.google.raw.decoder
com.google.
.com.google.android.apps.chrome.extra.cpu_count
1com.google.android.apps.chrome.extra.cpu_features
com.google.android.gms
Ccom.google.devtools.build.android.desugar.runtime.twr_disable_mimic
com.google.protobuf.Extension
%com.google.protobuf.ExtensionRegistry
dns.google
```

Replicant 6 WebView - 7 lines

```
1com.google.android.apps.chrome.extra.command_line
.com.google.android.apps.chrome.extra.cpu_count
1com.google.android.apps.chrome.extra.cpu_features
/com.google.android.apps.chrome.extra.extraFile_
'com.google.android.googlequicksearchbox
com.google.android.webview
%content://com.google.settings/partner
```

Approach #1: Stepwise cleansing

Still no 100% free-software WebView apk void of privacy concerns.

Tentative approach:

1. Start with Guix's source code for ungoogled-chromium.
2. Run Ubuntu's license check script on it.
3. Check if original Chromium bug about licensing still applies (was mostly related to third-party code).
4. Try to build WebView (will probably fail).
5. Cherry pick patches from ungoogled-chromium-android and Unobtainium.
6. Build everything in fdroid-server (picks leftover pre-builts).
7. Send recipe for peer-review at GNU-linux-libre.

Approach #2: WebView API compatibility shim for GeckoView

Chromium fork requires constant maintenance burden.

Google's interests do not align with ours. Check Mozilla.

GeckoView:

- Java wrapper for Gecko browser engine.
- Used in Android apps as replacement for WebView.
- API is incompatible with WebView: not meant to be a drop-in.

Mapping WebView to GeckoView

- Some functions have a 1:1 mapping.

WebView	GeckoView
`goBack()`, `goForward()`	`GeckoSession.NavigationDelegate`
`loadUrl()`	`GeckoSession.loadUri()`
`stopLoading()`	`GeckoSession.stop()`

Mapping WebView to GeckoView

- Some functions have a 1:1 mapping.

WebView	GeckoView
`goBack()`, `goForward()`	`GeckoSession.NavigationDelegate`
`loadUrl()`	`GeckoSession.loadUri()`
`stopLoading()`	`GeckoSession.stop()`

- Others require emulation.

WebView	GeckoView
`getTitle()`	`GeckoSession.HistoryDelegate.HistoryItem.getTitle()`
`pageDown()`	`PanZoomController.scrollBy(width,height)`

Mapping WebView to GeckoView

- Some functions have a 1:1 mapping.

WebView	GeckoView
`goBack()`, `goForward()`	`GeckoSession.NavigationDelegate`
`loadUrl()`	`GeckoSession.loadUri()`
`stopLoading()`	`GeckoSession.stop()`

- Others require emulation.

WebView	GeckoView
`getTitle()`	`GeckoSession.HistoryDelegate.HistoryItem.getTitle()`
`pageDown()`	`PanZoomController.scrollBy(width,height)`

- Others require more features from Gecko to be exposed via GeckoView, e.g. `zoomIn()`.

Mapping WebView to GeckoView

- Some functions have a 1:1 mapping.

WebView	GeckoView
`goBack()`, `goForward()`	`GeckoSession.NavigationDelegate`
`loadUrl()`	`GeckoSession.loadUri()`
`stopLoading()`	`GeckoSession.stop()`

- Others require emulation.

WebView	GeckoView
`getTitle()`	`GeckoSession.HistoryDelegate.HistoryItem.getTitle()`
`pageDown()`	`PanZoomController.scrollBy(width,height)`

- Others require more features from Gecko to be exposed via GeckoView, e.g. `zoomIn()`.

- Others still, added on latest Android APIs (26-29), seem too tied to Chromium, e.g. `getWebViewLooper()`, `getWebChromeClient()`, `getWebViewClient()`.

Mapping WebView to GeckoView

Requires a considerable effort.

Can pay off in the long-term: no need to constantly scout for proprietary dependencies and privacy issues.

Burden may be lessened by collaborations, e.g., qt5-webengine replacement with Gecko underneath.

Approach #3: GeckoView on apps

Fork apps to use GeckoView instead of WebView.

Impossible for the small Replicant team to maintain.

Would only work if app maintainers perceive GeckoView as a better alternative.

Feedback?

- Questions
- Comments
- Ideas
- Collaboration

All welcomed!

Licenses (I)

item	source	license
K-9 Mail logo	`https://github.com/k9mail/k-9`	Apache-2.0
OsmAnd logo	`https://github.com/osmandapp/Osmand`	CC-BY-NC-ND 4.0
Nextcloud logo	`https://github.com/nextcloud/android`	AGPLv3
Tiny Tiny RSS logo	`https://gitlab.com/derSchabi/tttrsss`	GPLv3
I2P logo	`https://github.com/i2p/i2p.android.base`	Apache-2.0
Orbot logo	`https://gitweb.torproject.org/orbot.git`	BSD
F-Droid logo	`https://gitlab.com/fdroid/fdroidclient`	GPLv3
andOTP logo	`https://github.com/andOTP/andOTP`	MIT
Shaarlier logo	`https://github.com/dimtion/Shaarlier`	GPLv3
wallabag logo	`https://github.com/wallabag/android-app`	GPLv3
OpenKeychain logo	`https://github.com/open-keychain/open-keychain`	GPLv3
EteSync logo	`https://github.com/etesync/android`	GPLv3
Syncthing logo	`https://github.com/syncthing/syncthing-android`	MPLv2
Briar logo	`https://code.briarproject.org/briar/briar`	GPLv3
Conversations logo	`https://github.com/siacs/Conversations`	GPLv3
Signal logo	`https://github.com/signalapp/Signal-Android`	GPLv3
Silence logo	`https://git.silence.dev/Silence/Silence-Android`	GPLv3
Tinc App logo	`https://github.com/pacien/tincapp`	GPLv3
KeePass DX logo	`https://github.com/Kunzisoft/KeePassDX`	GPLv3
dandelion* logo	`https://github.com/gsantner/dandelion`	GPLv3
Nomad logo	`https://framagit.org/disroot/AndHub`	GPLv3

Licenses (II)

item	source	license
Tusky logo	`https://github.com/tuskyapp/Tusky`	GPLv3
Movim logo	`https://github.com/movim/movim_android`	AGPLv3
Jami logo	`https://git.jami.net/savoirfairelinux/ring-client-android`	GPLv3
Bitmask logo	`https://0xacab.org/leap/bitmask_android`	GPLv3
WireGuard logo	`https://git.zx2c4.com/wireguard-android`	Apache-2.0
Fennec logo	`https://hg.mozilla.org/releases/mozilla-esr68`	MPL-2.0
Tor Browser logo	`https://gitweb.torproject.org/tor-browser.git`	MPL-2.0
Thorium logo	`https://github.com/sschueller/peertube-android`	AGPLv3
WebKit logo	`https://en.wikipedia.org/wiki/File:WebKit_logo_(2015).svg`	non-free
Chromium logo	`https://commons.wikimedia.org/wiki/File:Chromium_11_Logo.svg`	CC-BY 2.5
Replicant logo	`https://redmine.replicant.us/projects/replicant/wiki/Artwork`	CC-BY-SA 3.
Guix logo	`https://git.savannah.gnu.org/cgit/guix/guix-artwork.git/`	CC-BY-SA 4.
Bromite logo	`https://github.com/bromite/bromite.github.io`	GPLv3
Iridium logo	`https://github.com/iridium-browser/artwork`	non-free
Debian logo	`https://www.debian.org/logos/`	CC-BY-SA 3.
Unobtainium logo	`https://gitlab.com/thermatk/Unobtainium`	BSD
GeckoView logo	`https://github.com/mozilla/geckoview`	non-free
everything else	this slideshow	CC BY-SA 4.